components which can be used for generating a fingerprint file for verifying a buyer computer in future transactions;

ii) said buyer computer requesting to purchase merchandise from [to] said vendor server, said purchase request including said buyer computer's IP address;

iii) said buyer computer selecting a predetermined form of secured payment method;

i[ii]v) said payment method selection causing said vendor server to transmit to said security server a request for confirmation of said buyer computer's identity at said buyer computer's IP address;

[i]v) said confirmation request causing said security server to send a retrieval request to said IP address, said retrieval request including a retrieval program for detecting and retrieving said buyer's computer's fingerprint file, said retrieval request further comprising a response request asking for confirmation of said purchase request; whereby a positive response from said buyer's computer to said security server accompanied by said fingerprint file causes said security server to confirm said buyer computer's identity to said vendor server and to approve said purchase.

4) (Amended) A method of performing secure electronic transactions on a computer network, said network comprising a buying computer, an ISP computer and a vendor computer, including the steps of:

said ISP computer assigning to buying computer a Buyer-ID code said and IP address, said Buyer ID code being determined by said ISP computer after activating a diagnostic program to diagnose on a buying computer whether the buying computer has labeled components

2

which can be used for generating a fingerprint file for verifying a buying computer in future

transactions;

said buying computer communicating via said ISP computer with said vendor

computer and allowing an operator to select merchandise or services for purchase;

said Buyer-ID and buyer computer's IP address are provided to vendor computer

programmed to request and receive said information;

vendor computer is programmed to use Buyer-ID and [BC's] buyer computer's

current IP address along with information such as desired Item ID, cost and name for generating

an electronic purchase inquiry which is transmitted to ISP computer;

ISP is programmed such that upon receipt of purchase inquiry from [MC] vendor

computer, ISP uses combination of IP address and Buyer-ID to determine within ISP's internal

network whether buyer is in fact still online at the address assigned at the beginning of the online

session;

whereby if buyer computer is determined to be connected to ISP computer at

correct address, ISP computer then generates and transmits Transaction Confirmation Number

and instructs [MC] vendor computer to generate and forward invoice to ISP computer.


Please add the following new claims 5-15


5. (New) In a computer network, a system for performing a secured transaction

between a buyer's computer, a security server and one or more of a vendor server or a creditor

server, wherein a buyer's computer is provided with a buyer's identification code, said buyer's

3

identification code being adapted to be transmitted from said buyer's computer to said security server, said security server being adapted to compare the buyer's identification code with an assigned buyer's identification code, said security server being adapted to communicate with one of either a creditor server or a vendor the results of said comparison, said one of either a creditor server or said vendor server being adapted to complete a transaction based on the satisfactory comparison of said identification codes, said identification code including a fingerprint file, said finger print file being generated by one or more of a vendor server, a creditor server or a security server, said server having activated a diagnostic program to diagnose on a buyer computer whether the buyer computer has labeled components which can be used for generating a fingerprint file for verifying a buyer computer in future transactions.

6. (New) The network according to claim 5 wherein the buyer's computer is connected through an ISP to vendor's computer and wherein said security server is operated by said ISP.

7. (New) The network according to claim 6 wherein the identification code includes an internet protocol address.

8. (New) The network according to claim 7 wherein said internet protocol address remains constant throughout a transaction.

9. (New) The network according to claim 5 wherein said buyer's computer has

4.

received encryption programming and decryption programming from said security server.

10. (New) A method of performing secure electronic transactions on a computer network comprising

signing a buyer's computer into an ISP's computer, said buyer's computer having been assigned a buyer's identification code, said buyer's identification code being determined by said ISP activating a diagnostic program to diagnose on a buyer computer whether the buyer computer has labeled components which can be used for generating a fingerprint file for verifying a buyer computer in future transactions;

transmitting a message from a buyer's computer containing an identification code through said ISP's computer;

comparing the buyer's identification code with the assigned identification code;

connecting the buyer's computer through the ISP to a merchant's computer or a creditor's computer;

initiating a transaction between said buyer's computer and said merchant's computer or a creditor's computer, said merchant's computer or creditor's computer relying on the comparison of the buyer's identification code with the assigned identification code in said transaction.

11. (New) The method according to claim 10 wherein the transaction is initiated with a merchant's computer.

12. (New) The method according to claim 10 wherein the transaction is initiated with a creditor's computer.

13. (New) A method of performing a secured transaction between a buyer's computer a security server and one or more of a vendor server or a creditor server, comprising

providing a buyer's computer with a buyer's identification code, said buyer's identification code being determined by activating a diagnostic program to diagnose on a buyer computer whether the buyer computer has labeled components which can be used for generating a fingerprint file for verifying a buyer computer in future transactions;

transmitting said buyer's identification code being adapted from said buyer's computer to said security server,

said security server comparing the buyer's identification code with an assigned buyer's identification code;

said security server communicating with one of either a creditor server or a vendor the results of said comparison;

said one of either a creditor server or said vendor server completing a transaction based on the satisfactory comparison of said identification codes.

14. (New) The method according to claim 13 wherein the identification code includes an internet protocol address.

15. (New) The method according to claim 14 wherein said internet protocol

address remains constant throughout a transaction.

Respectfully submitted,

Thomas A. O'Rourke
Reg. No.: 27,665
BODNER & O'ROURKE, L.L.P.
425 Broadhollow Road
Melville, New York 11747
(631) 249-7500